

التحقيق في جرائم الحاسوب

القاضي. وليد عاكوم

شهد القرن الماضي ثورة من نوع غير مألوف اصطلح على تسميتها بثورة المعلومات، كـان بطلهـا جهاز الحاسب الآلي الذي تطور دوره بحيث تعدى إجراء العمليات الحسابية المعقدة ليشمل قضايا تُهم الناس في جميع معاملاتهم بما فيها قضايا الإتصالات مرورا بالمعلوماتية التوثيقية والذكاء الإصطناعي ألخ.

هذا التطور الكبير والمتسارع لدور الكمبيوتر ترافق مع تزايد الوعي لدى الشعوب لأهميـة المعلومـة بإعتبارها مصدرا للقوة والثروة أحيانا، لعل ما يدعم هذه الفكرة ويؤكدها هو تعمـيم اسـتخدام شـبكة الإنترنت على سكان الكرة الأرضية بصرف النظر عن عقائدهم وأيديولجياتهم وإنتمـاءاتهم الطائفيـة والعرقية، بعدما كان الهدف الأساسي لهذه الشبكة هو استعمالها لتلبية الحاجـات الحربيـة والدفاعيـة للولايات المتحدة الأمريكية.

ويمكن القول أيضا أن العقود الأخيرة من القرن العشرين شهدت فضلا عن ثورة المعلومـات، ثـورة جديدة في عالم الإتصال ونقل المعلومات مما اتاح للأفراد والمؤسسات فرصة الولوج إلى بنوك وقواعد المعلومات على الصعيدين المحلي والدولي، فانعكس هذا الأمر أيجابا على القطاعات الإقتصادية كمـا ألف مصدرا غنيا بالمعلومات لمراكز اتخاذ القرار.

ونتيجة هذا التطور في عالم المعوماتية نشأت ونمت أنواع جديدة من الجرائم التي ما كانـت لتبـصر النور لولا ظهور هذه الآلة التي اتفق على تسميتها بجهاز الكمبيوتر. هذه الجرائم تنوعـت واتخـذت مظاهر مختلفة بحيث أصبحت اليوم تطرح إشكاليات خطيرة على الصعيدين الإقتـصادي والقـانوني، فهي تشكل خطرا على التوظيفات والإستثمارات بسبب القرصنة مثلا، هذا من جهة، كما تستدعي فـي مراجعة شاملة للأحكام والنصوص القانونية، هذه المراجعة تظهر دون عنـاء أن القـوانين التقليديـة قاصرة على تغطية هذه الجرائم لأن تطبيق هذه القوانين يفترض وقوع الجرم على أموال مادية بينمـا جرائم المعلومات تقع على أموال معنوية لا تغطيها هذه القوانين.

ونشير في هذا المقام إلى أن هذه الجرائم الحديثة والمستحدثة تتنوع وتتضاعف يوما بعد يوم، ويختلف مرتكبوها عادة عن المجرمين التقليديين لأنهم في الغالب أشخاص علـى مـستوى عـال مـن العلـم والمعرفة.

وقد يكون بعضهم من صغار السن أي من طلاب المدارس الثانوية وحتى الإبتدائية أيضا هذا الوضـع يجعلنا بطبيعة الحال نخرج عن الإطار التقليدي للنظرة إلى المجرم العادي الذي نراه عادة في الأفـلام البوليسية وفي نظارات السجون.

- **وهؤلاء المجرمون يمكن تصنيفهم إلى الفئات التالية :**

1. **القراصنة** Les Pirates

** هناك صنفان من القراصنة :

- الصنف الاول : الهواة Hackers

وهم من الشباب الفضوليين الذين يسعون للتسلية ولا يشكلون خطـورة علـى الـصناعات وأنظمـة المعلومات.

- الصنف الثاني : المحترفون Crackers

وهم أكثر خطورة من الصنف الأول وقد يحدثون أضرارا كبيرة وقد يؤلفون أندية لتبادل المعلومـات فيما بينهم.

2. **المخادعون Fraudeurs**

وهؤلاء يتمتعون بقدرات فنية عالية بإعتبارهم عادة من الإخصائيين في المعلوماتية ومن أصـحاب الكفاءات، وتنصب معظم جرائمهم على شبكات تحويل الأمـوال ويمكـنهم التلاعـب بحـسابات المصارف أو فواتير الكهرباء والهاتف أو تزوير بطاقات الإعتماد أو ما شابه.

3. **الجواسيس** Espions

يهدف هؤلاء إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التـي تتنافس فيما بينهما.

ونظرا لحداثة تلك الجرائم ولتنوعها وللطابع التقني الذي يستخدم في إرتكابهـا، تواجـه الـسلطة القضائية والأجهزة الأمنية صعوبات عديدة في إكتشاف وملاحقة مرتكبيها[1].

** يدفع بنا هذا الأمر إلى التساؤل:

هل أن النصوص الجزائية التقليدية، موضوعية كانت ام إجرائية، كافية في مواجهة هـذا الـشكل المستحدث من الإجرام أم ان هذا الأمر يتطلب تدخلا تشريعيا لمواجهته حتى لا يفلت الجاني مـن العقاب؟

إجابة عن هذا التساؤل، لا بد من تحديد ماهية الجرائم المعلوماتية (اولا) ومن ثـم التطـرق إلـى القوانين المطبقة ودور الأجهزة الأمنية والقضائية في مواجهة هذه الجرائم (ثانيا).

- **أولا : ماهية الجرائم المعلوماتية:**

سوف نعالج، تحت هذا العنوان، مفهوم الجرائم المعلوماتية[2] والأشكال المختلفة التي يمكن ان ترتديها الإعتداءات على الإنظمة المعلوماتية[3].

---

(1) فتوح الشاذلي وعفيفي عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، 2003، ص 17.
(2) Hard ware.

1. مفهوم الجرائم المعلوماتية: يمكن تحديد مفهوم الجرائم المعلوماتية من منظارين:

أ- المنظار الأول : عندما تكون المعلوماتية موضوعا للإعتداء: وتتق هذه الحالة عندما تقع الجريمة على المكونات المادية للكمبيوتر من اجهزة ومعدات وكابلات وشبكات ربط وآلات طباعة وتصوير وغيرها أو عندما تقع على المكونات المعلوماتية أو غير المادية[4]. مثل البرامج المستخدمة والبيانات Data والمعطيات المخزنة في ذاكرة الكمبيوتر.

ب- المنظار الثاني: عندما تكون المعلوماتية أداة ووسيلة لإعتداء: وتتحقق هذه الحالة عندما يستخدم الجاني الكمبيوتر كوسيلة لتنفيذ جرائمه، سواء على الأشخاص كإنتهاك حرمة الحياة الخاصة[5] أو القتل[6]، او على الأموال كالسرقة والإحتيال والتزوير وغيرها، ويسمى هذا النوع من الجرائم "الاعمال الجرمية التي ترتكب بمساعدة الكمبيوتر".

وتتميز هذه الجرائم بصعوبة كشفها نظرا لإمكانية ارتكابها من مسافات بعيدة ولقدرة الجاني في تدمير الأدلة عليها في اقل من الثانية الواحدة وكونها لا تترك أي أثر مرئي.

2. **الاشكال المختلفة للاعتداءات على الأنظمة المعلوماتية:**

** يوجد نوعان من الإعتداءات على الأنظمة المعلوماتية:

أ. الإعتداءات المنطقية Attaques logiques

ب. الإعتداءات المادية Attaqes physiques

أ- **الإعتداءات المنطقية: وهي تشمل أنواعا عديدة، نكتفي بتعداد بعضها:**

- **الجرثومة المعلوماتية "أو" الفيروس : Virus Informatique**

أنه برنامج معلوماتي يتضمن أهدافا تدميرية لأنظمة المعلومات[7]. ويتميز بقدرته على نسخ نفسه في البرنامج الذي يصيبه، وبالتحكم به وتعديله، وبقدرته على تمييز البرامج المصابة بالعدوى وعدم تكرار إصابتها بالفيروس مرة اخرى.

ولدرء مخاطر الفيروسات المرسلة، تم صنع البرامج المضادة للفيروسات وبالرغم من ذلك، لا تزال الفيروسات تضرب مختلف قطاعات Anti virus– المعلوماتية وتتسلل إليها بواسطة البرامج المقرصنة.Pirate

---

(3) Soft ware

(4) Vie Privee – Privacy.

(5) كبرمجة جهاز تفجير والتحكم به آليا عن بعد.

(6) نزار فايز أبو علي، فيروسات الكمبيوتر، دار حنيني للنشر، عمان 1994.

(7) أو Hoax بالإنجليزية.

- **القنبلة المعلوماتية : Bombe informatique**

إنه برنامج يعده مصمم النظام المعلوماتي ويثبته بداخله بغية أن يعمل بعد انقضاء مدة محددة، على إستعمال النظام المعلوماتي بهدف تدميره أو تعطيلة او محو البيانات التي يحتويها.

- وهي على نوعين :

أ. القنبلة المنطقية logic Bomb وهي تهدف إلى تدمير المعلومات عند حدوث ظرف معين او لدى تغير أمر ما كشطب إسم أحد الموظفين مثلا.

ب. القنبلة الزمنية Time Bomb وهي تعمل في وقت محدد وفي يوم معين مثل فيروس shernobel الذي اكتشف عام 1998.

- **الدودة المعلوماتية : Worm-ver informatique**

أنه برنامج معلوماتي يمتاز بقدرته على التنقل عبر شبكات الإنترنت بهدف تعطيلها والتشويش عليها عبر شل قدرتها على التبادل.

- **الفخ أو الخبيئة :Trappe**

إنها نقطة دخول أو منفذ يجهز مسبقا في نظام معلوماتي من قبل مصممه، فيسمح له لاحقا بإنزال برامج خاصة من شأنها ان تعيق سير عمل هذا النظام المعلوماتي، وأن تدخل إليه عناصر إعاقة لتطبيقاته.

- **حصان طرواده: Cheval de Troie**

إنه برنامج يتضمن وظائف خفية يعرفها المعتدي وحده تسمح له بالالتفاف على أنظمة الأمن والمراقبة القائمة في هذا النظام.

- **الخداع(8): Mystification**

يهدف إلى الإيقاع "معلوماتيا" بمستعمل مرخص له بإستعمال نظام معلوماتي معين من اجل الإستيلاء على المعلومات المعرفة به التي تسمح له بالنفاذ إليه (كإسمه وكلمة المرور السرية...).

- **التسلل :Faufilement**

ويقضي بالتسلسل وراء مستعمل مرخص له بالدخول إلى نظام معلوماتي وتخطي نقطة مراقبة الدخول على هذا الشكل.

- **سلامي: Salami**

تسمح هذه التقنية بأخذ معلومات مجتزأة ومشتتة من نظام معلوماتي ومن ثم العمل على تجميعها وتركيبها تدريجيا.

(8) أو Trapping بالإنجليزية.

ب- الإعتداءات المادية: نذكر منها الإعتداءات الآتية:الإعتراض المتعمد للبيانات : Interception

ويقصد به رصد إشارات الكترومغناطسية في الأنظمة المعلوماتية بغية استخراج المعلومات المفهومـة أو المقروءة منها.

- **التشويش: Brouillage**

يهدف إلى إعاقة المستوى التشغيلي للأنظمة المعلوماتية وجعلها عاجزة عن العمل.

- التنصت: Ecoute

ويقوم على التمركز في موقع معين داخل شبكة الإتصالات، وتسجيل خفظ البيانات المتبادلة في ما بين الإنظمة المعلوماتية.

- التفخيخ [9]: Piegeage

ويحصل عندما يعمد المعتدي إلى إدخال وظائف خفية في مرحلة تصميم او تصنيع او نقل او صـيانة النظام المعلوماتية.

ويضاف إلى جميع الإعتداءات السالفة التي لا يمكن تعدادها وحصرها جريمة الإحتيـال المعلومـاتي، وهي تقوم على اتباع سلوك احتيالي او خداعلي مرتبط بالكمبيوتر يهدف شخص بواسطته إلى كـسب فائدة او مصلحة مالية.

وهذا يعني أن افعال الإحتيال التي تتحقق عن طريق حاسب آلي، والتي لا تستهدف مباشـرة "خـداع إنسان" لا تنفي إمكانية وجود أساليب إحتيالية.

بعد هذا التعداد المقتضب لبعض أنواع الجرائم المعلوماتية، ننتقل إلى دارسة القوانين المطبقـة علـى جرائم المعلوماتية ودور الأجهزة الأمنية في الكشف عنها.

- ثانيا: قمع الجرائم المعلوماتية:

ونبحث، تحت هذا الإطار، في دور الأجهزة في قمع ومكافحـة الجـرائم المعلوماتيـة[10]، وبعـض التطبيقات القانونية والقضائية في هذا المجال[11].

1. دور الاجهزة في مكافحة وقمع الجرائم المعلوماتية:

يختلف قمع ومكافحة الجرائم المعلوماتية عن ضبط الجرائم التقليدية، على اعتبار ان لهذه الجـرائم طبيعة خاصة إذ أن أدلتها غير محسوسة أو تحتاج مواجهتها إلى خبرات فنية وتقنية عالية.

إن مكافحة الجرائم مناط بالضابطة العدلية وبالقضاء، فيقتضي بالتالي التصدي إلى دور كل منهمـا في مكافحة الجريمة المعلوماتية.

---

(9) القاضي فوزي خميس، محاضرة بعنوان "جرائم المعلوماتية وحماية الملكية المعلوماتية وبنوك وقواعد المعلومـات، القيـت، بتاريخ 1999/2/25، وفي قاعة المحاضرات في نقابة المحامين في بيروت.

(10) هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة – أسيوط، ط 1994، ص 59 وما يليها.

(11) مثال على ذلك المادة 25 من قانون جريمة الحاسب الهولندي.



أ- دور الضابطة العدلية: يقتضي أن تقوم الضابطة العدلية (رجال قوى الأمن بشكل عام) بـدور هام في مكافحة الجرائم المعلوماتية على صعيدين:

- **مكافحة الجرائم المعلوماتية قبل وقوعها: الدور الوقائي:**

نظرا لطبيعة الجرائم المعلوماتية الخاصة، لا يستطيع عناصر الضابطة العدلية أن يؤدوا دورا إيجابيـا في هذا المجال.

إلا انه بالنظر إلى كون البرامج المعلوماتية تشكل قيما فكرية محمية بموجب القوانين الحديثة، يقتـصر دور رجال الضابطة العدلية في الحفاظ على هذه البرامج من النسخ غير المشروع عبر التأكـد مـن التزام المتعاملين في هذه البرامج بالحصول على ترخيص من مالكيها للتعامل بها.

ويتبلور دورها، على هذا الصعيد، عبر مراقبتها للمحلات التجارية، بواسطة وحدات متخصصة مـن عناصرها، للحؤول دون وقوع التعدي على برامج الحاسب الآلي أو لمنع استمراره.

- مكافحة الجرائم المعلوماتية بعد وقوعها: الدور القمعي:
- معاينة مسرح الجرائم المعلوماتية:

لا تواجه رجال الضابطة العدلية أي صعوبة تذكر عند معاينتهم لمسرح الجريمة الواقعة على المكونات المادية للكمبيوتر إذ أن مسرح الجريمة في هذه الحالة يحتوي على الأدلة الماديـة التـي تـدل دلالـة واضحة على وقوع الجريمة ونسبتها لشخص معين، فيقومون بعد ذلك بوضع الأختام وضـبط الأدلـة وإخطار النيابة العامة.

اما الصعوبات الحقيقية التي تواجه رجال الضابطة العدلية على هذا الصعيد، فتظهـر عنـدما تكـون الجريمة واقعة على برامج الكمبيوتر وبياناته او بواسطتها وذلك بالنظر إلى قلة الآثار المادية التي قـد تنتج عن هذا النوع من الجرائم وكثرة عدد الاشخاص الذين قد يترددون على مسرح الجريمة خـلال المدة الفاصلة بين وقوع الجريمة والكشف عنها.

- ويوصي[12]، في هذا الإطار، حفاظا على مسرح الجريمة، بما يأتي:

  - تصوير الكمبيوتر وما قد يتصل به من أجهزة بدقة تامة وأخذ صورة لأجزائه الخلفية وسائر ملحقاته.
  - ملاحظة طريقة إعداد نظام الكمبيوتر بعناية بالغة.
  - إثبات الحالة التي تكون عليها توصيلات وكابلات الكمبيوتر والمتصلة بمكونات النظام.
  - عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة خـشية إتـلاف البيانـات المخزنة.

---

(12) حول قرار قاضي التحقيق في بيروت، جريدة السفير العدد الصادر بتاريخ 1999/11/18، وحول قرار قاضي التحقيق فـي جبل لبنان، النشرة القضائية اللبنانية 1971 ص 488.



- **التفتيش عن أدلة الجريمة المعلوماتية:**

إذا كانت الجريمة واقعة على المكونات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش. أما إذا كانت الجريمة واقعة على برامج الحاسب وبياناته، فإن الصعوبات تبرز على إعتبار أنه بإمكان الجاني التخلص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر، وعلى اعتبار أن التفتيش عن هذه البيانات يستوجب الكشف عن الرقم السري code للمرور إلى ملفات البيانات، وهذا الرقم السري يعرفه المتهم، ولا يمكن اجباره على البوح به.

ومن أجل تخطي هذه الصعوبات، يجب برأينا أن لا يكون الاذن بالتفتيش محددا بمكان معين، بل يجب ان يمتد إلى تفتيش أي نظام آلي موجود في مكان اخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول في كشف الحقيقة، شرط عدم انتهاك سيادة دولة اخرى وان يحل قاضي التحقيق محل الشخص، صاحب المكان، المراد تفتيشه بصورة مؤقتة.

كما يجب أن يتضمن إذن التفتيش الاجازة بالبحث عن كيان البرنامج وأنظمة تشغيله والسجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات[13].

- **ضبط الأدلة:**

الضبط، بحسب الاصل، لا يرد إلا على اشياء مادية، فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر، كرفع البصمات مثلا عنها.

ولذلك، فلا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه غير المشروع أو إتلافه بوسائل تقليدية كالكسر أو الحرق.

ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وفي ضبط بيانات الكمبيوتر Data لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر او شفرات المرور او ترميز البيانات.

وبإنتظار استحداث قوانين تتضمن مفاهيما قانونية عامة وجديدة نقترح على هذا الصعيد ما يأتي:

- تشجيع المجني عليهم بالإبلاغ عن هذه الجرائم فور ملاحظتها.
- حث العاملين على النظام المعلوماتي على معاونة السلطة لضبط البيانات.
- ضرورة اتباع القواعد الفنية اللازمة لحماية البيانات وتجنيبها خطر الاتلاف.
- منح أوسع الصلاحيات لسلطة التحقيق لاختراق نظام الكمبيوتر وضبط ما يحويه من بيانات مخزنة دون إخطار مسبق بعملية التفتيش والضبط.

---

(13) قرار محكمة الجنايات منشور في مجلة العدل اللبنانية 2000 ص 375.

ب- دور السلطة القضائية:

على إعتبار أن القاضي هو حامي الحقوق والحريات، فإنه يجب أن يلعب دورا هاما في قمع الجرائم المعلوماتية.

وتفعيلا لهذا الدور، يجب على القاضي أن يكون متفهما لفحوى التقدم التقني وما ينتج عنها من وسائل اجرامية يغلب عليها الطابع التقني.

وعلى هذا الاساس، ينبغي أن يقبل بالأدلة المستمدة من الكمبيوتر لإثبات وقائع الدعوى التي تتناول جرائم المعلوماتية، ويساعده في هذا الامر مبدأ الإثبات الحر والقناعة الشخصية للقاضي في المجال الجنائي.

ومن ناحية اخرى، فإنه يجب أن يتحلى بالمقدرة على التكييف القانوني للأفعال الجرمية المستحدثة مع التشريعات التجريمية القائمة.

2. بعض التطبيقات القانونية والقضائية:

نعرض الآن الواقع القانوني والقضائي الذي يعالج الجرائم المعلوماتية كالآتي:

أ. القوانين المطبقة:

تتطلب الجرائم الواقعة على الأنظمة المعلوماتية أحكاما ونصوصا تجريمية خاصة بها.

وعليه، فقد بادرت العديد من الدول الغربية إلى وضع نصوص ومواد جزائية تعاقب صراحة الجرائم المعلوماتية، في حين أن القوانين في الدول العربية وفي لبنان خصوصا لم تتطرق بعد إلى هذه الفئة من الجرائم.

- في القانون اللبناني:

إن القانون اللبناني الوضعي الحالي لا يتطرق أبدا إلى الجرائم المعلوماتية بشكل مباشر، ولا تزال الدعاوى المتعلقة بهذه الجرائم تسند إلى المواد الجزائية التقليدية المنصوص عنها في قانون العقوبات.

فالتجسس معاقب عليه في قانون العقوبات اللبناني من المادة 281 لغاية المادة 284 عندما يطال المعلومات المتعلقة بسلامة الدولة فقط، ولا يتحدث عن حالات التجسس الصناعي او على الافراد، ولا يتمكن بالتالي التوسع في تفسير النص وجعله شاملا لهذه الحالات لأن القانون الجزائي يفسر بصورة ضيقة انطلاقا من مبدأ لا عقوبة دون نص.

أما التشويش والتخريب في أنظمة المعلومات، فيمكن الإستعانة بنص المادة 733 عقوبات التي تعاقب كل من خرب قصدا شيئا يخص غيره بالغرامة وبالحبس لغاية ستة أشهر، ولكن هذا النص يتعلق فقط بالاشياء الملموسة كأجهزة الكمبيوتر وتوابعها، ولا يتطرق إلى قضية التشويش والتخريب على المعلومات التي تحتويها.

أما المادة 635 عقوبات، فتعرف السرقة بأنها أخذ مال الغير المنقول خفية أو عنوة بقصد التملك، وتنزل الطاقات المحرزة منزلة الأشياء المنقولة في تطبيق هذا النص، ويستنتج من ذلك بأنه يمكن، بالاستناد إلى المادة المذكورة، معاقبة سارق جهاز الكمبيوتر كآلة، ولكن لا يمكن معاقبة سرقة المعلومات التي هي أشياء غير ملموسة.

أما الإبتزاز بإستعمال معلومات أمكن الحصول عليها عبر الأنظمة المعلوماتية، فتقع ضمن نطاق تطبيق نص المادة 650 عقوبات لأن النص المذكور لا يشير إلى مصدر المعلومات التي تستعمل في التهويل والإبتزاز.

وأن العقوبات الواردة في المادتين 471 و 454 عقوبات تطال تزوير بطاقات الإعتمادات المصرفية وإستعمالها كمستند – اما التزوير المعلوماتي أي تبديل الحقيقة على الشرائط الممغنطة وفي مجموعة البيانات اي على المضمون الذهني للبرامج، فلا يقع تحت أحكام هاتين المادتين لإنتفاء وجود المستند بالمعنى القانوني الوارد فيهما.

وبتاريخ 1999/4/13، صدر قانون متعلق بحماية الملكية الأدبية والفنية يحمل الرقم 75 ويعد هذا القانون إنجازا كبيرا في هذا المجال إذ انها المرة الأولى التي تعاقب بها الجرائم المعلوماتية بنص صريح.

فالمادة الأولى من القانون المذكور عرفت برنامج الحاسب الالي بما حرفيته: أنه مجموعة من الاوامر معبر عنها بكلمات او برموز او بأي شكل آخر بإمكانها عندما تدخل في مادة يمكن للحاسب أن يقرأها أن تجعل الحاسب الالي يؤدي أو ينفذ مهمة ما أو يعطي نتيجة ما.

كذلك، ورد في المادة الأولى تعريف لمسالة نقل المعلومات إلى الجمهور التي يمكن أن تكون موضوع مسألة إذا تناولت أعمالا مشمولة بالحماية وإذا جرت بواسطة وسائل سلكية او لا سلكية عن طريق الإنترنت.

واعتبر هذا القانون في المادة الثانية منه برامج الحاسب الآلي، مهما كانت لغات هذه البرامج، وكذلك الأعمال التحضيرية لهذه البرامج من ضمن الأعمال المشمولة بالحماية.

وقد أقرت المادتان 85 و 86 منه العقوبات اللازمة على كل من يعتدي على هذه البرامج.

- في قوانين الدول الغربية:

تعتبر فرنسا من بين أولى الدول التي أصدرت تشريعا خاصا في مجال الجرائم المعلوماتية بموجب قانونين: الاول، بتاريخ 1978/1/5 حول المعلوماتية والحريات، والثاني، فهو قانون Godfrain حول الغش المعلوماتي الصادر بتاريخ 1988/1/5.

ومن بين الإعتداءات التي أعطيت وصفا جرميا يعاقب عليه بالسجن وبغرامات مرتفعة، الدخول او البقاء غير المشروع داخل النظام المعلوماتي، والاعتداءات على المعلومات داخل الأنظمة، وجرائم التزوير في المعلوماتية، وتأليف جميعات الاشرار المعلوماتيين، وإدخال جراثيم أو ديدان أو القاء قنابل منطقة او احصنة طروادة وغيرها.

وضمن سياق الإجراءات والوسائل الوقائية لمواجهة جرائم المعلوماتية، أنشأت فرنسا ايضا، عام 2000، مكتبا مركزيا لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات تابعا لوزارة الداخلية الفرنسية.

أما الولايات المتحدة الأمريكية، فإصدرت في العام 1998 قانونيّن متخصصين بالجرائم المعلوماتية، هما "قانون الغش والتعسف في الكمبيوتر" Computer fraud and Abuse Act و "قانون سرية المخابرات الإلكترونية. Electronic communications Privacy Act

وكذلك، فلقد استخدث جهاز الـ FBI في العام 2000 المركز الخاص بمكافحة جرائم الإنترنت " حول كيفية مجابهة الجرائم المعلوماتية.

وعلى المستوى الأول، فلقد عقدت اجتماعات عديدة لبحث هذا الموضوع وصدرت توصيات وتقارير تختص بهذه الجرائم:

- في العام 1997 اجتماع مجموعة الدول الصناعية الثمانية حول "جرائم الشبكات" Cyber Criminalite or Crimes.
- في العام 2000، اجتماعان في باريس وفي أوكيناوا حول التعاون الدولي بوجه مجرمي الشبكات: Cyber Criminals
- لجنة اوجدها المجلس الأوروبي في العام 1997، حول الجرائم في فضاء الشبكات. Comite sur la criminalite dans le Cyberspace.

ب- تطبيقات قضائية في القانون اللبناني:

نذكر بعضها كالآتي:

- أقدم مستخدم، كان يعمل لدى شركة تتعاطى وضع البرامج المعلوماتية وبيعها من الغير، وبحكم إطلاعه على جميع برامج الشركة، إلى نسخ هذه البرامج واحتفظ بنسخ عنها في منزله، وبعد تقديم استقالته من الشركة، أقدم على عرض هذه البرامج للبيع إلى عدة زبائن بسعر زهيد، فأقامت عليه الشركة دعوى جزائية. فأدانه القاضي المنفرد الجزائي بجرمي المادتين 70+2 تقليد - علامة فارقة – و 714 عقوبات مزاحمة احتيالية.
- ولكن محكمة الإستئناف فسخت الحكم الإبتدائي لجهة جرم تقليد العلامة الفارقة لأن البرامج لم تكن مسجلة في دائرة حماية الملكية التجارية والصناعية، وذلك بصرف النظر عما إذا كانت هذه البرامج قابلة للتسجيل أم لا، وصدقته لجهة التجريم بجرم المزاحمة الإحتيالية.
- في مطلع شهر تشرين الثاني من العام 1999، أصدر قاضي التحقيق في بيروت قرارا ظنيا في قضية سرقة اسطوانات حاسب آلي تحوي قيود السجل العقاري لدى المديرية العامة للشؤون العقارية بهدف استثمارها والمتاجرة بها.

فأعتبر ان إستنساخ المعلومات الموجودة بداخل "الهارديسك" الموجود في الحاسب الآلي في مديرية الشؤون العقارية لا يعد سرقة لأنه لم يجر الإستيلاء عليه ككيان مادي.

كما أعتبر أن السرقة بمدلولها القانوني غير متوفرة لأنه لم يجر "أخذ الهارديسك"، ولم ينقل من مكانه، ولم يدخل في حيازة أحد من المدعي عليهم، بل اجرى استنساخ المعلومات الموجودة بداخله وهو بمكانه في الحاسب الآلي، وبالتالي لم يجر الإستيلاء عليه بصفته مالا منقولا بكيانه المادي، مما ينفي بالنتيجة تحقق أحد الأركان الأساسية لجرم السرقة المنصوص عنه في المادة 638 عقوبات.

وقد استشهد القاضي المذكور بحالة تطبيقية سبق أن عرض لها قاضي ا لتحقيق في جبل لبنان- وهي تشبه حالة تصوير المستند المذكورة اعلاه – عندما قرر عدم توفر أركان جرم السرقة بحق طلاب دخلوا إلى مدرستهم في غياب المسؤولين عنها وتمكنوا من الوصول إلى غرفة الإدارة، ثم أخذوا من الخزانة أسئلة الإمتحان أو نسخوها، معللا ذلك بأن المدعي عليهم الطلاب أقدموا على سرقة الأسئلة عن طريق نسخها من دون أن يسرقوا الورقة المكتوب عليها تلك الأسئلة والتي وحدها لها الكيان المادي(14).

- وبتاريخ 2000/4/26، تجنبت محكمة الجنايات في بيروت الخوض في نقاش الوصف القانوني لجرم "السرقة"، معتبرة أن نسخ المعلومات العقارية المخزنة داخل "الهارديسك" يؤلف اعتداء على اثر فكري محمي، وطبقت عقوبة النسخ غير المشروع لبرنامج الحاسب الآلي المنصوص عنها في قانون حماية الملكية الأدبية والفنية(15).

ولكن محكمة الجنايات في بيروت قد خلطت في قرارها بين برنامج الحاسب الآلي الذي أدرجه قانون الملكية الادبية والفنية في لائحة الأعمال الفكرية المشمولة بالحماية التي يقررها هذا القانون، وبين المعلومات غير المادية المدخلة والموثقة في ذاكرة الحاسب الآلي التي قد لا يستحوذ بالضرورة على هذا الوصف، وكذلك خلط بين مفهوم برامج الحاسب الآلي، ومجموعات الأعمال المعلوماتية، مما يدل على النقص في استيعاب القضاء للجوانب التقنية لهذه المؤلفات الجديدة(16).

- وكذلك واجه القضاء اللبناني قضية فيها تعرض كبير للآداب العامة والأخلاق العامة تمكن من معالجتها رغم حصولها في شبكة الإنترنت بحيث تمكنت السلطات الأمنية اللبنانية بالتعاون مع الإنتربول من توقيف شخص لبناني كان يبث صورا خلاعية للأطفال وذلك بأمر من النيابة العامة، التي أحالته إلى قاضي التحقيق في بيروت الذي ظن فيه بالمواد 531 و 532 و 533 عقوبات وفقا لمطالعة النيابة العامة، وأحاله أمام القاضي المنفرد الجزائي في بيروت الذي أدانه سندا للمواد المذكورة.

ولكن محكمة الإستئناف الجزائية عادت وفسخت الحكم إذا أعتبرت أن عناصر الجرم المنصوص عنه في المادتين 531 و532 غير متوفرة بسبب عدم توفر شرط العلنية للجمهور المنصوص فيه في المادة 209 عقوبات، ولكنها أدانته سندا للمادة 533 عقوبات فقط.

(14) حول قرار قاضي التحقيق في بيروت، جريدة السفير العدد الصادر بتاريخ 1999/11/18، وحول قرار قاضي التحقيق في جبل لبنان، النشرة القضائية اللبنانية 1971 ص 488

(15) قرار محكمة الجنايات منشور في مجلة العدل اللبنانية 2000 ص 375.

(16) طوني عيسى، المرجع المذكور سابقا، ص 1890.

ولكننا نخالف ما قضت به محكمة الإستئناف على اعتبار ان بث الصور والمشاهد الخلاعية عبر شبكة الإنترنت عرضة للالتقاط من ملايين المشاهدين، إذ يكون شرط العلنية متوافرا.

- وبتاريخ 2001/2/12، أدان القاضي المنفرد الجزائي في كسروان بجرم التقليد شخصا أقدم على نقل وتقليد معلومات موضوعة على أسطوانات مرنة Floppy Disk تخص الشركة المدعية.
- وبتاريخ 2001/10/11، أدان القاضي المنفرد الجزائي في المتن بموجب المادة 733 عقوبات شخصا بسبب دخوله إلى مركز الشرطة حيث كان يعمل على الحاسب الآلي بغفلة عن احد زملائه السابقين وأقدامه على انتزاع اجزاء مهمة منه وإخفائها في مركز العمل في أمكنة غير مرئية، مما أدى إلى تعطيل العمل في الشركة بضعة ساعات قبل العثور على الأجزاء المفقودة.

الخاتمة

يتبين من مجمل هذه الدراسة أن القوانين التقليدية المعمول بها عاجزة وقاصرة عن مكافحة الجرائم المعلوماتية بشكل مباشر.

- لذلك، نوصي ببعض المقترحات، وهي الآتية:

1. ضرورة إستحداث قواعد مناسبة في مجال الإجراءات الجنائية بشأن التحقيق في الجرائم المعلوماتية.
2. العمل على تكوين فريق متخصص من الأجهزة الأمنية يكلف بالبحث والتحري عن هذا النوع من الجرائم وإجراء دورات تدريبية بصورة مستمرة.
3. إعتبار المال المعلوماتي المعنوي على قدم المساواة في الحماية الجنائية مع الأموال المنصوص عنها في قوانين العقوبات التقليدية والإعتراف بإمكان اتلاف هذا المال وتقرير العقوبة عنها المقررة اصلا على إتلاف المال المادي.
4. إنشاء مركز قومي لأمان الحاسبات والمعلومات وضمان عدم إصابتها بالفيروس.
5. ضرورة التعاون الدولي لمواجهة هذا النوع من الإجرام.



المراجع

- **المراجع العربية:**

1. فتوح الشاذلي وعفيفي عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، 2003.
2. طوني عيسى، التنظيم القانوني لشبكة الإنترنت، منشورات صادر الحقوقية، 2001.
3. نزار فايز أبو علي، فيروسات الكمبيوتر، دار حنين للنشر، عمان 1994.
4. فوزي خميس، جرائم المعلوماتية وحماية الملكية المعلوماتية وبنـوك وقواعـد المعلومـات، محاضرة ألقيت في نقابة المحامين في بيروت بتاريخ 1999/2/25.
5. هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثـة – أسـيوط 1994.
6. منصور مغايرة، دراسة حول "الجرائم المعلوماتية"، مكتبة جامعة الحكمة، 1999-2000.

- **المراجع الاجنبية :**

1. Martin, la Criminalite inforatique, P.U.K. 1997.
2. Champy, la fraude informatique, Proses universitaires d' Aix – Marseille 1996.

- **الدوريات القانونية:**

1. مجلة العدل، تصدر عن نقابة المحامين في لبنان.
2. النشرة القضائية، تصدر عن وزارة العدل في لبنان.